Journal of Number Theory **93**, 76–85 (2002)
doi:10.1006/jnth.2001.2714, available online at http://www.idealibrary.com on IDEAL®

A Note on Algebraic Γ-Monomials and Double Coverings

Soogil Seo

School of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455

Communicated by G. W. Anderson

Received January 18, 2001

We discuss algebraic Γ-monomials of Deligne. Deligne used the theory of Hodge Cycles to show that algebraic Γ-monomials generate Kummer extensions of certain cyclotomic fields. Das, using a double complex of Anderson and Deligne's results, showed that certain powers of algebraic Γ-monomials and certain square roots of sine monomials generate abelian extensions of $\mathbb{Q}$. Das also gave one example of a nonabelian double covering of a cyclotomic field generated by the square root of a sine monomial. In this note, we will produce infinitely many examples of non-abelian double coverings of cyclotomic fields of Das type. The construction of the examples depends in an interesting way on a lemma of Gauss figuring in an elementary proof of quadratic reciprocity.

1. INTRODUCTION

Let $\mathbb{A}$ be the free abelian group generated by the symbols $[a]$, where $a \in \mathbb{Q}/\mathbb{Z}$. Let $\mathbb{U}$ be the quotient of $\mathbb{A}$ by the subgroup generated by all elements of the form $[a]-\sum_{nb=a}[b]$, $n \in \mathbb{N}$ and $a \in \mathbb{Q}/\mathbb{Z}$. Let $\mathbb{U}^-$ be the quotient of $\mathbb{U}$ by the elements of the form $[a]+[-a]$. We recall that the Γ-function is defined by

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$$

and satisfies the following functional equations:

$$\Gamma(s)\Gamma(1-s) = \pi(\sin \pi s)^{-1}$$

$$\Gamma(1+s) = s\Gamma(s).$$

0022-314X/02 $35.00

For each a in $\mathbb{Q}/\mathbb{Z}$, let $\langle a\rangle$ be the smallest positive rational number representing the class of a in $\mathbb{Q}/\mathbb{Z}$. Let $\mathbf{a} = \sum m_i[a_i] \in \mathbb{A}$. Let f be the lcm of the denominators of the $\langle a_i\rangle$. We define

$$\tilde{\Gamma}(\mathbf{a}) = (2\pi i)^{-\sum m_i \langle a_i\rangle} \prod_{a_i \neq 0} \Gamma(\langle a_i\rangle)^{m_i},$$

cf. [4]. We define the Γ-monomial

$$\Gamma(\mathbf{a}) = \prod_{a_i \neq 0} \left(\frac{\sqrt{2\pi}}{\Gamma(\langle a_i\rangle)}\right)^{m_i}$$

and the sine monomial

$$\sin \mathbf{a} = \prod_{a_i \neq 0} (2 \sin \pi\langle a_i\rangle)^{m_i},$$

cf. [2]. Let $\mathbb{Q}^{alg}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and let $\mathbb{Q}^{ab}$ be the maximal abelian field in $\mathbb{Q}^{alg}$. Let μ_n be the set of nth roots of unity in $\mathbb{Q}^{ab}$ and let $\zeta_n = \exp(2\pi i/n) \in \mu_n$.

Koblitz and Ogus (cf. Appendix of [3]) found a sufficient condition for $\tilde{\Gamma}(\mathbf{a})$ to be algebraic:

$$\sum m_i\langle a_i\rangle = \sum m_i\langle ta_i\rangle, \qquad \text{for all} \quad t \in (\mathbb{Z}/f\mathbb{Z})^\times \Rightarrow \tilde{\Gamma}(\mathbf{a}) \in \mathbb{Q}^{alg}.$$

Abusing notation, we write $\mathbf{a} \in H^2(\pm, \mathbb{U})$ if $\mathbf{a}$ represents an element of $H^2(\pm, \mathbb{U})$, the latter identified with a subgroup of $\mathbb{U}^-$ as

$$H^2(\pm, \mathbb{U}) = \frac{\ker(1-c : \mathbb{U} \to \mathbb{U})}{\text{image}(1+c : \mathbb{U} \to \mathbb{U})} \subset \frac{\mathbb{U}}{\text{image}(1+c : \mathbb{U} \to \mathbb{U})} = \mathbb{U}^-,$$

where c is the involution of $\mathbb{U}$ induced by $[a] \mapsto [-a] : \mathbb{A} \to \mathbb{A}$. We denote the torsion subgroup of $\mathbb{U}^-$ by $\mathbb{U}^-_{tor}$. It was proven by Kubert that $\mathbb{U}$ is a free abelian group and $\mathbb{U}^-_{tor} = H^2(\pm, \mathbb{U})$ and in effect that the hypothesis of the Koblitz–Ogus criterion is equivalent to $\mathbf{a} \in H^2(\pm, \mathbb{U})$. By the theorem [4, Theorem 7.15, p. 91] of Deligne, if $\mathbf{a} = \sum m_i[a_i] \in H^2(\pm, \mathbb{U})$ and $\sum m_i\langle a_i\rangle$ is an integer, then $\tilde{\Gamma}(\mathbf{a})$ is not only algebraic but also generates a Kummer extension of $\mathbb{Q}(\mu_f)$. When $\mathbf{a} = \sum m_i[a_i] \in H^2(\pm, \mathbb{U})$ and f is odd, Das found the following relations (Theorem 15 of [2]):

$$\Gamma(\mathbf{a})^{2f} = \sqrt{r}\, \sin^f \mathbf{a}, \qquad \text{for some rational number } r \in \mathbb{Q}$$

and

$$\tilde{\Gamma}(\mathbf{a})\, i^{(\sum m_i \langle a_i \rangle)} = \Gamma(\mathbf{a})^{-1}.$$

(It is easy to show that $(\sum m_i \langle a_i \rangle)$ is an integer in this case.) Thus, in particular, Das reproved in an elementary way the fact that $\tilde{\Gamma}(\mathbf{a})$ generates a Kummer extension of $\mathbb{Q}(\mu_f)$. Note from the above equation that the Galois structure of the field generated by $\tilde{\Gamma}(\mathbf{a})$ is nearly the same as the Galois structure of the field generated by $\Gamma(\mathbf{a})$ over $\mathbb{Q}$.

Given a Galois extension K/k, we define a *double covering* (cf. [2]) of K/k to be a field extension $\tilde{K}/K$ of degree $\leqslant 2$ such that $\tilde{K}/k$ is Galois. Das (Section 8 of [2]) gave a basis for $H^2(\pm, \mathbb{U})$ indexed by finite sets consisting of an even number of prime numbers. Let $H^2(\pm, \mathbb{U})_{\geqslant 4}$ be the subspace spanned by the elements of Das's basis indexed by sets of 4 or more odd primes. Das found that if f is odd then $\mathbf{a} \in H^2(\pm, \mathbb{U})$ gives rise to double coverings of $\mathbb{Q}(\mu_f)/\mathbb{Q}$ by $\mathbb{Q}(\mu_f, \Gamma(\mathbf{a})^f)$, $\mathbb{Q}(\mu_f, \sqrt{\sin \mathbf{a}}\,)$ and

$$\mathbf{a} \in H^2(\pm, \mathbb{U})_{\geqslant 4} \Rightarrow \Gamma(\mathbf{a})^f, \sqrt{\sin \mathbf{a}} \in \mathbb{Q}^{ab}.$$

For each pair of odd primes $p < q$, put

$$\begin{aligned}\mathbf{a}_{pq} = &\sum_{i=1}^{(p-1)/2} \left([i/p] - \sum_{k=0}^{(q-1)/2} \left[\frac{i/p+k}{q} \right] \right) \\ &- \sum_{j=1}^{(q-1)/2} \left([j/q] - \sum_{l=0}^{(p-1)/2} \left[\frac{j/q+l}{p} \right] \right) \in \mathbb{A}.\end{aligned}$$

Then $\mathbf{a}_{pq}$ represents the element of Das's basis indexed by $\{p, q\}$. Das showed that $\mathbb{Q}(\mu_{60}, \sqrt{\sin \mathbf{a}_{3,5}})/\mathbb{Q}$ is nonabelian. We show that the extension $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})/\mathbb{Q}$ is nonabelian for infinitely many p, q. Under certain quadratic residue conditions we also show that $\mathbb{Q}(\mu_{pq}, \tilde{\Gamma}(\mathbf{a}_{pq}))$ and $\mathbb{Q}(\mu_{pq}, \Gamma(\mathbf{a}_{pq}))$ are nonabelian Galois extensions of $\mathbb{Q}$ and we determine the smallest integer m such that $\Gamma(\mathbf{a}_{pq})^m$ and ζ_{4pq} generate a nonabelian extension of $\mathbb{Q}$. More precisely, we have the following theorem.

THEOREM A. *For all odd primes $p < q$, if $(\frac{q}{p}) = -1$ or $(\frac{p}{q}) = -1$, then the extensions $\mathbb{Q}(\mu_{pq}, \tilde{\Gamma}(\mathbf{a}_{pq})^{pq})/\mathbb{Q}$ and $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})/\mathbb{Q}$ are Galois and nonabelian.*

2. MAIN RESULTS

We define the *universal ordinary distribution* $\mathbb{U}$ to be the free abelian group generated by symbols $\{[a] \mid a \in \mathbb{Q}/\mathbb{Z}\}$ with relations $[a] = \sum_{nb=a} [b]$,

$a \in \mathbb{Q}/\mathbb{Z}$, $n \in \mathbb{N}$ and the *universal odd distribution* $\mathbb{U}^-$ to be the quotient of $\mathbb{U}$ by the relations $[-a] = -[a]$, $a \in \mathbb{Q}/\mathbb{Z}$. As in the introduction, we identify the cohomology group $H^2(\pm, \mathbb{U})$ with a subgroup of $\mathbb{U}^-$. It was proven by Kubert that $\mathbb{U}$ is a free abelian group and $\mathbb{U}^-_{tor} = H^2(\pm, \mathbb{U})$ and in effect that the hypothesis of the Koblitz–Ogus criterion is equivalent to $\mathbf{a} \in H^2(\pm, \mathbb{U})$. Deligne [4] showed that if $\mathbf{a} = \sum m_i [a_i] \in H^2(\pm, \mathbb{U})$, then $\tilde{\Gamma}(\mathbf{a})$ is not only algebraic but also generates a Kummer extension of $\mathbb{Q}(\mu_f)$ provided that $\sum m_i \langle a_i \rangle$ is an integer.

Let $\mathbb{Q}^{ab}$ be the maximal abelian extension in a fixed algebraic closure $\mathbb{Q}^{alg}$. For each odd prime p let v_p, $v_{\mathfrak{p}}$ be additive valuations of $\mathbb{Q}^{ab}$ such that $v_p(p) = 1$, $v_{\mathfrak{p}}(1 - \zeta_p) = 1$. The following Lemma is fundamental in the paper and will be frequently used. It follows immediately from the Kronecker–Weber theorem.

LEMMA 2.1. *For each $a \in \mathbb{Q}^{ab}$, one has $v_p(a) \in (p-1)^{-1} p^{-\infty}\mathbb{Z}$, $v_{\mathfrak{p}}(a) \in p^{-\infty}\mathbb{Z}$.*

Lemma 2.1 is useful to check that a field is abelian.

EXAMPLE. Let p, q be distinct odd primes. We claim that the splitting field of $x^4 - p^a q^b$ is nonabelian over $\mathbb{Q}$ if $a \equiv 3 \bmod 4$ or $b \equiv 3 \bmod 4$. Suppose, say, that $a \equiv 3 \bmod 4$. Let v_p be any additive valuation of $\mathbb{Q}^{alg}$ above p such that $v_p(p) = 1$. Then for any root α of $x^4 - p^a q^b$, we have $v_p(\alpha) = \frac{a}{4}$ and hence $\alpha \notin \mathbb{Q}^{ab}$ by Lemma 2.1.

For odd primes $p < q$ put

$$\mathbf{a}_{pq} = \sum_{i=1}^{(p-1)/2} \left([i/p] - \sum_{k=0}^{(q-1)/2} \left[\frac{i/p+k}{q} \right] \right) - \sum_{j=1}^{(q-1)/2} \left([j/q] - \sum_{l=0}^{(p-1)/2} \left[\frac{j/q+l}{p} \right] \right),$$

as in the Introduction. Recall the family $\{\mathbf{a}_{pq}\}$ forms part of a basis for $H^2(\pm, \mathbb{U})$. Note that the theorem of Deligne [4, Theorem 7.15, p. 91] asserts that $\mathbb{Q}(\tilde{\Gamma}(\mathbf{a}), \zeta_f)$ and $\mathbb{Q}(\tilde{\Gamma}(\mathbf{a})^f, \zeta_f)$ are Galois extensions of $\mathbb{Q}$. The first application of Lemma 2.1 is the following proposition.

PROPOSITION 2.2. *$\mathbb{Q}(\mu_{pq}, \tilde{\Gamma}(\mathbf{a}_{pq}))$ is a nonabelian extension of $\mathbb{Q}$.*

Proof. It suffices to show that $\mathbb{Q}(\mu_{pq}, \Gamma(\mathbf{a}_{pq}))$ is a nonabelian extension of $\mathbb{Q}$. Suppose that $\mathbb{Q}(\mu_{pq}, \Gamma(\mathbf{a}_{pq}))$ is an abelian extension of $\mathbb{Q}$. We start with the following equation (Section 9 of [2]),

$$\Gamma(\mathbf{a}_{pq})^{2pq} = q^{(p-1)^2 q/8} p^{-(q-1)^2 p/8} \sin^{pq} \mathbf{a}_{pq}.$$

By Lemma 2.1, if K is abelian, then $v_{\mathfrak{p}}(a) \in p^{-\infty}\mathbb{Z}$. From the equation $\Gamma(\mathbf{a}_{pq})^{2pq} = q^{(p-1)^2 q/8} p^{-(q-1)^2 p/8} \sin^{pq} \mathbf{a}_{pq}$ we have

$$\Gamma(\mathbf{a}_{pq}) = \zeta\, q^{(p-1)^2/16p} p^{-(q-1)^2/16q} \sin^{1/2} \mathbf{a}_{pq}, \quad \text{for some} \quad \zeta \in \mu_{2pq}.$$

Recall that $q > p$. Then

$$v_{\mathfrak{p}}(\Gamma(\mathbf{a}_{pq})) = \frac{n}{mq},$$

for some $m, n \in \mathbb{Z}$, $(n, q) = 1$. This contradicts Lemma 2.1. ∎

Let $(\frac{p}{q})$ be the quadratic residue symbol.

PROPOSITION 2.3. *For odd primes $p < q$, we have*

$$\left(\frac{p}{q}\right) = (-1)^{v_{\mathfrak{q}}(\sin(\mathbf{a}_{pq}))} \text{ and } \left(\frac{q}{p}\right) = (-1)^{v_{\mathfrak{p}}(\sin(\mathbf{a}_{pq}))},$$

where $v_{\mathfrak{p}}$ is any valuation of $\mathbb{Q}^{ab}$ above p such that $v_{\mathfrak{p}}(1-\zeta_p) = 1$ and $v_{\mathfrak{q}}$ is analogously chosen valuation above q.

Proof. For all relatively prime integers r, s with $r > 0$ and square free,

$$v_{\mathfrak{p}}\left(2 \sin\left(\frac{\pi s}{r}\right)\right) = \begin{cases} 1 & \text{if} \quad p = r, \\ 0 & \text{if} \quad p \neq r. \end{cases}$$

Hence to compute $v_{\mathfrak{p}} \sin(\pi \frac{i/p+k}{q})$(resp. $v_{\mathfrak{q}} \sin(\pi \frac{j/q+k}{p})$), we need only check whether $i+kp$(resp. $j+qk$) is divisible by q (resp. divisible by p). We recall the sine monomial $\sin \mathbf{a}$ for $\mathbf{a} = \sum_i m_i[a_i] \in \mathbb{A} : \sin \mathbf{a} = \prod_{a_i \neq 0} (2 \sin \pi\langle a_i \rangle)^{m_i}$. We compute

$$v_{\mathfrak{p}}(\sin \mathbf{a}_{pq}) = \frac{p-1}{2} - \sum_{i=1}^{(p-1)/2} \sum_{k=0}^{(q-1)/2} v_{\mathfrak{p}} \sin\left(\pi \frac{i/p+k}{q}\right)$$

and

$$v_{\mathfrak{q}}(\sin \mathbf{a}_{pq}) = \frac{q-1}{2} - \sum_{j=1}^{(q-1)/2} \sum_{l=0}^{(p-1)/2} v_{\mathfrak{q}} \sin\left(\pi \frac{j/q+k}{p}\right).$$

We observe that

$$\sum_{i=1}^{(p-1)/2} \sum_{k=0}^{(q-1)/2} v_{\mathfrak{p}} \sin\left(\pi \frac{i/p+k}{q}\right) = \#\left\{(i, k) \;\middle|\; \begin{array}{c} kp \equiv -i \bmod q, \\ 1 \leqslant i \leqslant (p-1)/2, \\ \text{and } 1 \leqslant k \leqslant (q-1)/2 \end{array}\right\}$$

$$= \# \left\{ (i, k) \;\middle|\; \begin{array}{c} i+kp = qx, \\ 1 \leqslant i \leqslant (p-1)/2, \\ 1 \leqslant x \leqslant (p-1)/2, \\ \text{and } 1 \leqslant k \leqslant (q-1)/2 \end{array} \right\}$$

$$= \# \left\{ i \;\middle|\; \begin{array}{c} i \equiv qx \bmod p, \\ 1 \leqslant i \leqslant (p-1)/2, \\ \text{and } 1 \leqslant x \leqslant (p-1)/2 \end{array} \right\}.$$

We need Gauss's Lemma which is as follows:

Let p be an odd prime and n an integer with $(n, p) = 1$. Let S denote the set of least positive residues of the integers $n, 2n, ..., \frac{1}{2}(p-1)\, n$. Let r denote the number of elements of S which exceed $p/2$. Then $(\frac{n}{p}) = (-1)^r$.

Write

$$s(\mathfrak{p}) = \sum_{i=1}^{(p-1)/2} \sum_{k=0}^{(q-1)/2} v_{\mathfrak{p}} \sin\left(\frac{i/p+k}{q}\right)$$

and

$$s(\mathfrak{q}) = \sum_{j=1}^{(q-1)/2} \sum_{l=0}^{(p-1)/2} v_{\mathfrak{q}} \sin\left(\frac{j/q+l}{p}\right).$$

Then from the Gauss Lemma we have

$$(-1)^{s(\mathfrak{p})} = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) \qquad \text{and} \qquad (-1)^{s(\mathfrak{q})} = (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Hence from

$$v_{\mathfrak{p}}(\sin \mathbf{a}_{pq}) = \frac{p-1}{2} - s(\mathfrak{p}) \qquad \text{and} \qquad v_{\mathfrak{q}}(\sin \mathbf{a}_{pq}) = \frac{q-1}{2} - s(\mathfrak{q}),$$

one can find easily that

$$\left(\frac{p}{q}\right) = (-1)^{v_{\mathfrak{q}}(\sin(\mathbf{a}_{pq}))}, \qquad \left(\frac{q}{p}\right) = (-1)^{v_{\mathfrak{p}}(\sin(\mathbf{a}_{pq}))}. \quad \blacksquare$$

The main application of Lemma 2.1 is the following theorem.

THEOREM 2.4. *If* $(\frac{q}{p}) = -1$ *or* $(\frac{p}{q}) = -1$, *then* $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})$ *is a nonabelian extension of* $\mathbb{Q}$.

Proof. We apply Lemma 2.1 and Proposition 2.3 to conclude that the extension $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})$ is a nonabelian extension of $\mathbb{Q}$. ∎

Proposition 2.3 and Lemma 2.1 give us the following proposition.

PROPOSITION 2.5. *If* $(\frac{q}{p}) = -1$ *or* $(\frac{p}{q}) = -1$, *then* $\mathbb{Q}(\mu_{pq}, \tilde{\Gamma}(\mathbf{a}_{pq})^{pq})$ *and* $\mathbb{Q}(\mu_{pq}, \Gamma(\mathbf{a}_{pq})^{pq})$ *are nonabelian extensions of* $\mathbb{Q}$.

Proof. We fix a prime ideals $\mathfrak{P}$ over $\mathfrak{p} = (1-\zeta_p)$ and $\mathfrak{Q}$ over $\mathfrak{q} = (1-\zeta_q)$ of q in $\mathbb{Q}(\mu_{pq})$. Write $p = \pm 1 + 4s$ and $q = \pm 1 + 4t$. Since $p = \mathfrak{P}^{p-1}\mathfrak{A}$, $q = \mathfrak{Q}^{q-1}\mathfrak{B}$, for some $\mathfrak{A}$, $\mathfrak{B}$ with $(\mathfrak{A}, \mathfrak{P}) = 1$ and $(\mathfrak{B}, \mathfrak{Q}) = 1$, the identity $\Gamma(\mathbf{a}_{pq})^{2pq} = q^{(p-1)^2 q/8} p^{-(q-1)^2 p/8} \sin^{pq} \mathbf{a}_{pq} = \alpha \sin^{pq} \mathbf{a}_{pq}$ can be written

$$p = 1+4s, \qquad q = 1+4t,$$
$$\Gamma(\mathbf{a}_{pq})^{2pq} = \mathfrak{Q}^{2sq(q-1)}\mathfrak{P}^{-2tp(p-1)}\mathfrak{A}^*\mathfrak{B}^* \sin^{pq} \mathbf{a}_{pq}.$$
$$p = 1+4s, \qquad q = -1+4t,$$
$$\Gamma(\mathbf{a}_{pq})^{2pq} = \mathfrak{Q}^{2sq(q-1)}\mathfrak{P}^{(-2t^2-2t+1)\, p(2s)}\mathfrak{A}^*\mathfrak{B}^* \sin^{pq} \mathbf{a}_{pq}.$$
$$p = -1+4s, \qquad q = 1+4t,$$
$$\Gamma(\mathbf{a}_{pq})^{2pq} = \mathfrak{Q}^{(2s^2-2s+1)\, q(2t)}\mathfrak{P}^{-2tp(p-1)}\mathfrak{A}^*\mathfrak{B}^* \sin^{pq} \mathbf{a}_{pq}.$$
$$p = -1+4s, \qquad q = -1+4t,$$
$$\Gamma(\mathbf{a}_{pq})^{2pq} = \mathfrak{Q}^{(2s^2-2s+1)\, q(2t-1)}\mathfrak{P}^{(-2t^2-2t+1)\, p(2s-1)}\mathfrak{A}^*\mathfrak{B}^* \sin^{pq} \mathbf{a}_{pq}.$$

For the first three cases we get from Proposition 2.3,

$$2v_{\mathfrak{p}}(\Gamma(\mathbf{a}_{pq})^{pq}) = 1 \mod 2 \qquad \text{or} \qquad 2v_{\mathfrak{q}}(\Gamma(\mathbf{a}_{pq})^{pq}) = 1 \mod 2.$$

For the last case $p = -1+4s$, $q = -1+4t$, from the proof of Proposition 2.3, we have either

$$2v_{\mathfrak{p}}(\sin \mathbf{a}_{pq}) = 0 \mod 2 \qquad \text{and} \qquad 2v_{\mathfrak{q}}(\sin \mathbf{a}_{pq}) = 1 \mod 2,$$

or

$$2v_{\mathfrak{p}}(\sin \mathbf{a}_{pq}) = 1 \mod 2 \qquad \text{and} \qquad 2v_{\mathfrak{q}}(\sin \mathbf{a}_{pq}) = 0 \mod 2,$$

hence for this case we also have

$$2v_{\mathfrak{p}}(\Gamma(\mathbf{a}_{pq})^{pq}) = 1 \mod 2, \qquad \text{or} \qquad 2v_{\mathfrak{q}}(\Gamma(\mathbf{a}_{pq})^{pq}) = 1 \mod 2.$$

From Lemma 2.1, $\mathbb{Q}(\mu_{pq}, \Gamma(\mathbf{a}_{pq})^{pq})$ is a nonabelian extension of $\mathbb{Q}$. ∎

Remark. We write $\alpha = q^{(p-1)^2 q/8} p^{-(q-1)^2 p/8}$. Then for each $\mathbf{a}_{pq}$, we can write $\Gamma(\mathbf{a}_{pq})^{2pq} = \alpha \sin^{pq} \mathbf{a}_{pq}$. We have the following diagram of field extensions.

$$\begin{tikzcd}
 & k(\sqrt{\alpha}, \sqrt{\sin \mathbf{a}_{pq}}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & k(\Gamma(\mathbf{a}_{pq})) \arrow[dl, dash] \\
k(\sqrt{\alpha}) \arrow[dr, dash] & k(\sqrt{\sin \mathbf{a}_{pq}}) \arrow[d, dash] & k(\Gamma(\mathbf{a}_{pq})^{pq}) = k(\sqrt{\alpha}\sqrt{\sin \mathbf{a}_{pq}}) \arrow[dl, dash] & \\
 & k = \mathbb{Q}(\mu_{4pq}) \arrow[d, dash] & & \\
 & \mathbb{Q} & &
\end{tikzcd}$$

Note that when $p, q = 1 \mod 4$, we have $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}}) = \mathbb{Q}(\mu_{4pq}, \Gamma(\mathbf{a}_{pq})^{pq})$. It is clear from the equation $\Gamma(\mathbf{a}_{pq})^{2pq} = q^{(p-1)^2 q/8} p^{-(q-1)^2 p/8} \sin^{pq} \mathbf{a}_{pq}$ that $\tilde{\Gamma}(\mathbf{a}_{pq})^{2pq}$ generates an abelian extension. Therefore pq is the smallest integer m such that $G(\mu_{4pq}, \tilde{\Gamma}(\mathbf{a}_{pq})^m)$ is abelian.

3. SOME CONDITIONS FOR $G(\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})/\mathbb{Q})$ TO BE NONABELIAN

In this final section we provide some necessary and sufficient conditions for $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})$ and $\mathbb{Q}(\mu_{4pq}, \Gamma(\mathbf{a}_{pq})^{pq})$ to be nonabelian over $\mathbb{Q}$.

LEMMA 3.1. *Let $k = \mathbb{Q}(\mu_n)$ and $K = k(\sqrt{\alpha})$, $\alpha \in k$, a quadratic extension of k. Suppose that K is an abelian extension of $\mathbb{Q}$. Assume that α has even multiplicities at all primes of k, i.e., $v_{\mathfrak{p}}(\alpha) \in 2\mathbb{Z}$ for all primes $\mathfrak{p}$ of k.*

Then

$$K = \begin{cases} \mathbb{Q}(\mu_{4n}),\ \mathbb{Q}(\mu_{pq}, \sqrt{\pm 2}\,) & \text{when } 4 \nmid n \\ \mathbb{Q}(\mu_{2n}) & \text{when } 4 \mid n. \end{cases}$$

Moreover if α *is unit at primes over* 2 *and* $4 \nmid n$ *then we get* $K = \mathbb{Q}(\mu_{4n})$.

Proof. Let $\mathbb{Q}(\mu_m)$ be the smallest cyclotomic field containing K. Using the Hensel's lemma, K/k is unramified at all odd primes and the infinite prime. If K/k is unramified at the primes over 2, then we have

$$K = k = \mathbb{Q}(\mu_n)$$

since the Galois group $G(\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_n))$ is generated by the inertia groups. Hence K/k is ramified at a prime over 2 and $m = 2^r n$. By the structures of the Galois groups, K is equal to one of the following fields.

$$\mathbb{Q}(\mu_n, \sqrt{\pm 2}\,),\ \mathbb{Q}(\mu_{4n}) \qquad \text{when} \quad 4 \nmid n,$$

$$\mathbb{Q}(\mu_{2n}) \qquad \text{when} \quad 4 \mid n.$$

Suppose now that α is unit at primes over 2 and $4 \nmid n$. If $K = \mathbb{Q}(\mu_n, \sqrt{\pm 2}\,)$, then

$$\sqrt{\alpha} = \beta\sqrt{2}\,, \text{ or } \sqrt{\alpha} = \beta\sqrt{-2}\,, \text{ for some } \beta \in \mathbb{Q}(\mu_n).$$

If $\sqrt{\alpha} = \beta\sqrt{\pm 2}$ then the primes over 2 ramify in $\mathbb{Q}(\mu_n)/\mathbb{Q}$, since $\sqrt{\alpha}$ is unit at the primes over 2. If $4 \nmid n$, then it is impossible. This completes the proof. ▮

PROPOSITION 3.2. $[\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}}) : \mathbb{Q}(\mu_{4pq})] = 2$ *if and only if the Galois group* $G(\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})/\mathbb{Q})$ *is nonabelian.*

Proof. One implication is trivial. We prove that if $[\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}}) : \mathbb{Q}(\mu_{4pq})] = 2$ then $G(\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})/\mathbb{Q})$ is nonabelian. If $(\frac{q}{p}) = -1$ or $(\frac{p}{q}) = -1$, then this is true by Theorem 2.4. We assume that $(\frac{p}{q}) = (\frac{q}{p}) = 1$ and $[\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}}) : \mathbb{Q}(\mu_{4pq})] = 2$. Suppose that $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})$ is an abelian extension of $\mathbb{Q}$. Then we have that $[\mathbb{Q}(\mu_{pq}, \sqrt{\sin \mathbf{a}_{pq}}) : \mathbb{Q}(\mu_{pq})] = 2$. From Proposition 2.3, $\sin \mathbf{a}_{pq}$ has even multiplicities at all primes of $\mathbb{Q}(\mu_{pq})$. Now applying Lemma 3.1, with $\alpha = \sin \mathbf{a}_{pq}$, unit at primes over 2, $k = \mathbb{Q}(\mu_{pq})$, we have $\mathbb{Q}(\mu_{pq}, \sqrt{\sin \mathbf{a}_{pq}}) = \mathbb{Q}(\mu_{4pq})$. This is a contradiction to $[\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}}) : \mathbb{Q}(\mu_{4pq})] = 2$. Hence $\mathbb{Q}(\mu_{4pq}, \sqrt{\sin \mathbf{a}_{pq}})$ is nonabelian extension of $\mathbb{Q}$. ▮

ACKNOWLEDGMENTS

We thank Greg Anderson for introducing this area of research and for his numerous discussions and comments on it. It was suggested by him to the author that there might be a connection between the problem given here and the quadratic residue symbols, in particular, the Gauss Lemma. This suggestion led to the present paper. We thank the referee for helpful comments and suggestions.

REFERENCES

1. G. W. Anderson, A double complex for computing the sign-cohomology of the universal ordinary distribution, *in* “Recent Progress in Algebra,” Contemp. Math., Vol. 224, pp. 1–27, Amer. Math. Soc., Providence, 1999.
2. P. Das, Algebraic Gamma monomials and coverings of cyclotomic fields, *Trans. Amer. Math. Soc.* **352** (2000), 3557–3594.
3. P. Deligne, Valeurs de fonctions L et périodes d’intégrales, *in* “Proc. Sympos. Pure Math.,” Vol. 33, Part 2, pp. 343–346, Amer. Math. Soc., Providence, 1979.
4. P. Deligne, J. S. Milne, A. Ogus, and K.-Y. Shih, “Hodge Cycles, Motives and Shimura Varieties,” Lecture Notes in Math., Vol. 900, Springer-Verlag, New York, 1982.
5. D. S. Kubert, The universal ordinary distribution, *Bull. Soc. Math. France* **107** (1979), 179–202.
6. D. S. Kubert, The $\mathbb{Z}/2\mathbb{Z}$ cohomology of the universal ordinary distribution, *Bull. Soc. Math. France* **107** (1979), 203–224.
7. S. Lang, “Cyclotomic Fields,” Graduate Texts in Mathematics, Springer-Verlag, New York/Berlin, 1990.
8. W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math. (2)* **108** (1978), 107–134.
9. L. Washington, “Introduction to Cyclotomic Fields,” Graduate Texts in Mathematics, Springer-Verlag, New York/Berlin, 1982.

Printed in Belgium